

CLAIMS

1. An apparatus for determining in a global network the user status as the user goes from site to site within said network, said apparatus comprising:
 - 5 a set of baseline authentication agencies responsible for core global network authentication services;
 - a global network domain and associated DNS records used for cookie sharing, login routing, and the like; and
- 10 a collection of partner sites with access to cookies shared via said global network domain.

2. The apparatus of Claim 1, wherein a baseline authentication agency of said set of baseline authentication agencies:
 - 15 provides authentication services for a subset of the users of the global network after authenticating a user, writes a site identification along with an authenticated status of true into a cookie of said global network domain shared and accessible by said collection of partner sites; and when a global network user logs out of said global network, resets the user's authenticated status to false in said 20 shared domain cookie.
3. The apparatus of Claim 2, further comprising means for when an authenticated global network user using a browser visits a partner site of said collection of partner sites, said partner site accessing said shared 25 domain cookie to determine the user's baseline authentication agency;

means for said partner site redirecting said user's browser to said baseline authentication agency to request global network id informational of the user;

wherein said baseline authentication agency distinguishes between sites that have been linked and that have a trust relationship with the user and ones that have
5 not been linked; and

means for said baseline authentication agency returning said global network id informational of the user to said partner site if it's a linked site, thereby performing a seamless authentication, and if said site is not linked, said baseline authentication agency returning an authentication error indication.

10

4. The apparatus of Claim 2, further comprising:

means for when an unauthenticated global network user visits a global partner site, said global network partner site attempting to access said shared domain cookie and either not finding said cookie at all, or determining that said authenticated status
15 is false; and

wherein in either case, said global network partner site determining that a user is not authenticated into the global network and thus not allowing access for said user.

20 5. The apparatus of Claim 2, further comprising a globally unique identifier for each global network user account, wherein said globally unique identifier is a primary key with which global network user data records are indexed, and wherein for privacy reasons, only said globally unique identifier and a name of an associated baseline authenticating agency are shared with third party sites unless a user opts-in
25 to distributing said global network login id.

6. The apparatus of Claim 1, further comprising means for decentralizing core global network functionality, said means for decentralizing further comprising:

means for propagating selected global network user information to global network partner sites by setting cookies on a global network domain for which each 5 partner has an entry, such that partners can fetch said data without hitting any centralized global network server.

7. A method for an existing global network user using a browser and having a global network account logging onto a global network partner site without preexisting 10 authentication, said user having an account on said partner site, wherein said user account has an account number, and wherein said user previously authorized said global network to seamlessly log said user into said partner site, said method comprising the steps of:

15 said user authenticating itself to a baseline authentication agency associated with the user, via any suitable method allowed by said baseline authentication agency and said global network;

20 said baseline authentication agency setting values of a plurality of shared cookies, said plurality of cookies set on a partner-site-accessible subdomain of a global network domain, thereby readable by said baseline authentication agency and all global network partner sites, said plurality of shared cookies comprising, but not limited to:

a shared network login status cookie containing both the user's global network login status, and the network id of the user's baseline authentication agency;

25 said baseline authentication agency setting values of a plurality of private cookies, set on a private domain only accessible by said baseline authentication agency, said plurality of private cookies comprising, but not limited to:

one or more global network credential cookies;

 said baseline authentication agency generating a short-lived, partner-specific, encrypted login token and returning it to the browser as a hidden input field in an auto-submitting input form;

5 said browser processing said auto-submitting input form returned by said baseline authentication agency and submitting said login token to a partner site's login handler;

 said partner site performing a server to server token validation request to said baseline authentication agency by passing said login token;

10 said baseline authentication agency validating said login token and returning the user's global network account number to the partner site; and

 said partner site mapping the user's global network account number to a corresponding login id on said partner site, proceeding to log in, setting corresponding cookies on said partner site, and returning a personalized welcome
15 page to said browser.

8. The method of Claim 7, wherein at least one cookie of said plurality of cookies serves as a flag to said partner sites indicating that the user is logged into the global network.

20

9. The method of Claim 7, wherein said global network server generates a short-lived, partner site-specific, encrypted global network login token, and wherein a response of said global network server comprises a redirect instruction to said partner site global for a network login handler, and wherein said redirect instruction
25 comprises said global network login token.

10. A method for a user on a global network using a browser visiting a partner Web site, wherein said partner Web site is a linked and seamlessly login enabling global network site, during an ongoing session, said method comprising the steps of:

5 said user selecting said partner Web site and said browser requesting a home page of said partner Web site, wherein said home page of said partner Web site comprises a JavaScript tag telling said browser to fetch a partner site-served JavaScript file from said partner site server, as well as fetch other relevant JavaScript code;

10 said partner Web site server obtains a network login status cookie on a global network domain, thereby determining said user's global network login status and BAA;

15 said partner Web site using a BAA id from said network login status cookie for formulating a URL to a login token-generation service of said associated authentication agency domain, and returning an HTTP redirect to said URL;

20 said browser fetching said URL, and passing a global network site id of said partner Web site;

25 said associated authentication agency domain receiving said token-generation request including said site id, as well as any corresponding user global network credential cookie previously sent to the browser;

30 said partner Web site's home page comprising a particular JavaScript code and using said particular JavaScript code for determining a JavaScript login-token variable has a value, wherein if said login-token variable has said value, then said proceeds with a seamless global network login processing;

35 said partner Web site requesting mapping of said login-token variable to an user global network account number;

5 said global network server decrypting said login-token variable and performing validation checks on said login-token variable, said checks comprising, but not limited to: not expired and if an associated IP of said requesting partner Web site is in an allowed list, and if said validation checks pass, then said global network server returning said global network account number to said partner Web site; and

10 said partner Web site mapping said user's global network account number to a corresponding partner Web site record, logging user in, setting cookies of said partner Web site, and returning a personalized welcome page.

15 11. The method of Claim of 10 further comprising the steps of:

20 said associated authentication agency domain checking if the site id is known or valid, if said user's credentials are valid, and if the user has authorized seamless login to said partner Web site.

15 12. The method of Claim of 10, said seamless global network login processing further comprising the steps of:

25 said JavaScript code writing out an HTML form comprising said global network login token as a hidden field and writing out a partner Web site global network login handler as an action URL, and auto-submitting said form such that said browser posts said form to said partner Web site global network login handler URL on said partner Web site.